REMARKS/ARGUMENT

This Amendment and the following remarks are intended to fully respond to the Office Action mailed August 10, 2007, hereinafter "Office Action". In that Office Action claims 1-9 and 18-22 were examined, and all claims were rejected. More specifically, claims 18-22 were rejected under 35 U.S.C. § 101 because the office action asserts the claims are directed to non-statutory subject matter; and claims 1-9 and 18-22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Faucher (USPN 5,515,441), hereinafter "Faucher" in view of Inoue et al. (USPN 6,170,057), hereinafter "Inoue."

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested.

In this Response, claims 1, and 18-22 have been amended, new claims 26 and 27 have been added, and no claims have been canceled. Therefore, claims 1-9, 18-22, and 26-27 remain present for examination.

Interview Summary

Applicants thank Examiner Klimach for the in person interview with Applicants' representatives conducted on December 13, 2007. In that interview, the differences between the claims and the Faucher reference were discussed. No agreement was reached. Also discussed were the documents recently filed under-seal pursuant to MPEP § 724.02.

Claim Rejections – 35 U.S.C. § 101

Claims 18-22 were rejected under 35 U.S.C. § 101 because the office action asserts the claims are directed to non-statutory subject matter. Claims 18-22 have been amended to recite a computer storage medium. The specification states,

> "Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any

other medium which can be used to store the desired information and which can be accessed by the computer 110." (Specification, p. 6, line 24 – p. 7, line 1)

The embodiments recited in the amended claims are encoded in tangible, computer-readable media and are, thus, patentable subject matter under 35 U.S.C. § 101. *In re Beauregard*, 53 F.3d 1583, 1584 (Fed. Cir. 1995). Applicant's respectfully request that the Examiner withdraw the § 101 rejection and issue a notice of allowance for all claims.

Claim Rejections – 35 U.S.C. § 103(a)

Claims 1-9 and 18-22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Faucher in view of Inoue. Applicants respectfully traverse the § 103(a) rejections because either the Examiner failed to state a *prima facie* case of obviousness or the current amendments to the claims now render the Examiner's arguments moot. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Neither Faucher nor Inoue, either separately or in combination, teach or suggest all of the limitations of the recited claims.

Faucher relates to a communication system in which a node may communicate over insecure channels by securing communications. Communications are secured by computing a first cryptovariable from information associated with certificates exchanged between a node and a terminal, computing a second cryptovariable using public key exchange, and computing a session cryptovariable as a function of the first and second cryptovariables. (Faucher, Abstract, *See also* col. 9, l. 6 – col. 10, l. 16).

Faucher fails suggest conducting a main mode negotiation for establishing the secure path and selecting the set of security parameters including a security protocol; and conducting a quick mode negotiation for deriving a set of keys usable with the security protocol, as recited in claim 1. During the December 13, 2007 interview, the Examiner maintained that the calculation of the first session key in Faucher constituted a "main mode" and the calculation of the second

session key in Faucher constituted a "quick mode." Applicants disagree; however, even if Faucher did teach conducting a main mode negotiation and conducting a quick mode negotiation, the reference still fails to teach or suggest all of the limitations of independent claim 1.

For example, Faucher also fails to teach or suggest: wherein at least one message that comprises *at least part of the quick mode negotiation is sent during the main mode negotiation* and a quick mode pseudo random number is exchanged between the responder and the initiator. (emphasis added). As discussed above, Faucher teaches generating a first session key using information contained in certificates passed between the computing devices. (*See* Faucher, col. 9, l. 66 – col. 10, l. 13). Second, Faucher discloses generating a second session key with a "straight Diffie-Hellman key exchange." (Faucher, col. 10, ll. 13-15). However, at no point does the reference teach or suggest that a least one message that comprises at least part of the Diffie-Hellman key exchange used to create the second session key is sent during the certificate exchange used to create the first session key. In fact, Faucher teaches just the opposite: "[The first session key is calculated], thus validating the remote terminal. The procedure *continues* with a straight Diffie-Hellman key exchange to generate a second session key." (See Faucher, col. 10, ll. 2-15, emphasis added). Thus, the reference fails to teach or suggest, at least, wherein at least one message that comprises *at least part of the quick mode negotiation is sent during the main mode negotiation* and a quick mode pseudo random number is exchanged between the responder and the initiator.

Inoue fails to compensate for Faucher's deficiencies. Inoue relates to a packet encryption and authentication method capable of controlling an activation of a packet encryption and authentication device belonging to a mobile computer. The device is controlled according to the security policy of the network that the mobile computer is visiting. (*See* Inoue, Abstract). Inoue teaches that when a mobile computer recognizes that it is located outside of its home network, it acquires the security parameters associated with the gateway of the home network and the security parameters of the gateway associated with the network currently being visited by the mobile computer. (*See* Inoue, col. 7, ll. 20-27). As such, Inoue also fails to disclose a main mode or quick mode negotiation at all, and it cannot be used to overcome the deficiencies of Faucher. In light of at least these deficiencies, claim 1 is allowable over the cited references.

For at least similar reasons, independent claim 18 is also allowable over the cited references. Claim 18 recites, *inter alia*,

> conducting a main mode negotiation for establishing the secure path and selecting the set of security parameters including a security protocol;
>
> conducting a quick mode negotiation for deriving a set of keys usable with the security protocol;
>
> wherein at least one message that comprises at least part of the quick mode negotiation is sent during the main mode negotiation and a quick mode pseudo random number is exchanged between the responder and the initiator. . . .

New independent claims 26 and 27 also contain elements that are not taught or suggested in the cited references. Therefore Applicants submit that the claims are allowable and respectfully request that the Examiner issue a notice of allowance for new claims 26 and 27.

For at least the forgoing reasons, neither Faucher nor Inoue, alone or in combination, teach all of the limitations of independent claims 1 and 18, and claims 1 and 18 are allowable over the references of record. All other claims, *i.e.*, claims 2-9 and 19-22 depend from one of the allowable independent claims and are, thus, also allowable over the cited references. New claims 26 and 27 are also allowable over the cited references. Therefore, Applicants respectfully request that the Examiner issue a notice of allowance, for all claims, at her earliest convenience.

Conclusion

This Amendment fully responds to the Office Action mailed on August 10, 2007. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicant believes the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the art of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: January 10, 2008

Gregory D. Leibold, Reg. No. 36,408
Merchant & Gould P.C.
PO Box 2903
Minneapolis, MN 55402-0903
303.357.1642